

なぜ今、被害公表が相次ぐのか

2026年秋のインシデント集中を読み解くレポート

— AIの高度化 / 対策投資の空白 / 取引先経由の侵入 —

本文中の数値はすべて公表済みの一次情報に基づく（出典は巻末）

EGセキュアソリューションズ株式会社

<https://www.eg-secure.co.jp/>

目次

- 1 何が起きているか — 2026年秋の公表
- 2 要因1 — AIによる攻撃の高速化
- 3 要因2 — 守る側の「投資の空白」
- 4 要因3 — 取引先・委託先経由の侵入
- 5 3つが重なると何が起きるか
- 6 何から着手するか
- 7 事実と推測の区分・本レポートの限界

要旨

2026年9月下旬から10月上旬にかけて、国内の大規模インシデント公表が続けに起きた。個別に見れば業種も手口も異なるが、背景には共通する3つの構造変化がある。

-7日

62.6%

78%

脆弱性の公表（多くはパッチ公開
と同時）から悪用までの平均日
数（＝脆弱性の公表より前に悪用が始
まる）

直近3期にセキュリティ投資を
していない中小企業

国内ランサムウェア被害の
うち資本金10億円未満の組織

この3つが同時に起きている

1. 攻撃の速度が上がった。

AIで攻撃工程が自動化され、パッチが出るより前に悪用が始まるのが平均的な状態になった。実例として、人間なら2週間かかる侵入工程が10時間未満に圧縮された事案が報告されている。

2. 守る側に投資の空白がある。

直近3期にセキュリティ投資をしていない中小企業は62.6%。最多の理由は「必要性を感じていない」。一方で国内ランサムウェア被害の78%は資本金10億円未満の組織が占める。

3. 侵入口が自社の外に移った。

委託先・SaaS経由の侵害が相次ぎ、委託先1社の侵害が、取引先9組織に及んだ例もある。自社の防御水準は、つながっている中で最も弱い組織の水準に引き下げられる。

示唆

攻撃コストが下がると、これまで「狙うには割に合わない」とされた規模・業種が標的に入る。「うちは狙われるほど大きくない」という前提と、「パッチを当てれば間に合う」という運用の前提が、ともに2026年に崩れた。問うべきは「自社が狙われているか」ではなく「自社が何とつながっているか」である。

1 何が起きているか 2026年秋の公表

この10日間に公表された、国内の主なインシデント。件数はいずれも各社公表時点の値であり、調査中のものを含む。

10日間で5件。2026年秋の公表



図：10日間で5件。赤は委託先・外部サービスが起点の事案

● 委託先・外部サービスが起点の事案 ● 自社システムで起きた事案

公表	組織	概要	規模
9/26	京王電鉄グループ	ランサムウェア攻撃でサーバー障害。 ホテル・百貨店・ストア・バス等に影響。 鉄道運行への支障はなし	漏えい件数は未公表
9/28	タイムズモビリティ (パーク24)	不正アクセス。 氏名・住所・運転免許情報等。うち本人確認書類の 画像 約160万件。 原因は調査中	約660万アカウント
10/2	第一生命 (第一ライフグループ ／第一生命)	人事システムへの不正アクセス (9/24検知)。 従業員・退職者の氏名・住所・所属・上長名等。 約12万人のうち約7万人が退職者。 顧客情報への被害は未確認	約12万人分 (従業員)
10/4	日本経済新聞社	社員のMicrosoft 365アカウント乗っ取り。 なりすましメール約9,000件を送信。 別途Google Workspaceから漏えいのおそれ	1,646人分 (ほか調査中)

公表	組織	概要	規模
10/5	大和証券	委託先スカラコミュニケーションズのサーバーへの不正アクセス。 自社システムへの侵入は未確認	約22万件 (うち個人情報 約11万人分)
10/5～	スカラコミュニケーションズ (FAQシステム委託先)	管理サイトへの不正ログイン→同一サーバー上の他社DBから取得。 大和証券・シチズン時計・損保ジャパン・東武鉄道が影響を公表	最大713,126件 (最大5社分)
8月～	両毛システムズ (IT委託先)	VPNアカウント悪用による侵入→ランサムウェア。 ガス事業者8社+自治体1件(計9組織)に波及	約12.4万件 (大東ガス分)

※ 京王電鉄グループの事案は情報漏えいではなく「事業継続への影響」型。日本経済新聞社の「約9,000件」は漏えい件数ではなく、なりすましメールの送信件数（漏えい件数は調査中）。第一生命の約12万人分は顧客ではなく従業員・退職者の人事情報。報道見出しの数字をそのまま並べると性質を取り違えるため、本表では区別して記載した。

侵害はどこで起きたのか。

6件中4件は 従来の防御 が見ていなかった場所

大和証券 侵害箇所 委託先のサーバー 補足情報 スカラコミュニケーションズ	大東ガス ほか8組織 侵害箇所 委託先のIT企業 補足情報 両毛システムズ/VPN悪用	日本経済新聞社 侵害箇所 業務用クラウド 補足情報 Microsoft 365アカウント
第一生命 侵害箇所 社内の人事システム 補足情報 顧客システムとは別系統	タイムズモビリティ 侵害箇所 調査中 補足情報 侵入経路は未公表	京王電鉄グループ 侵害箇所 調査中 補足情報 漏えいは未確認

図：侵害が起きた場所。従来の防御が見ていなかった場所

■ 自社が直接管理していない場所、または自社の防御の想定外にあった場所

この一覧から読めること

6件のうち**4件は、従来の防御が見ていなかった場所**で侵害が起きている — 委託先サーバー、クラウドの業務アカウント、社内の人事システム。「外から壁を破られた」のではなく、「すでに内側につながっていた経路」が使われた。

2 要因1 — AIによる攻撃の高速化

2-1. 脆弱性は「量」より「速度」が変わった

Google Threat Intelligence Group (GTIG) の2026年9月30日レポートによれば、月間の脆弱性 (CVE) 公表件数は**2026年1月の5,045件から、同年8月には10,740件へと倍増した**。

ただしGTIG自身が「この生の件数は誤解を招く」と注記している。自動採番による水増しが相当数含まれ、実際に悪用されたのは公表された脆弱性の**わずか0.23% (約431件に1件)**にとどまる。件数の倍増それ自体を脅威の倍増と読むのは誤りである。

意味があるのは、悪用の「中身」のほうだ。

- **公表かつ悪用された脆弱性は2026年1～8月で141件**。2025年通年の127件を、8か月ですでに超えた (月平均 10.5件 → 18件)。
- **リスクの高い脆弱性の悪用は2025年通年28件 → 2026年1～8月で75件と2倍超**。
- CVE公表からCISA KEV (既知悪用脆弱性カタログ) 入りまでの中央値は、**2025年の120日から2026年上半期は80日へ短縮 (VulnCheck)**。

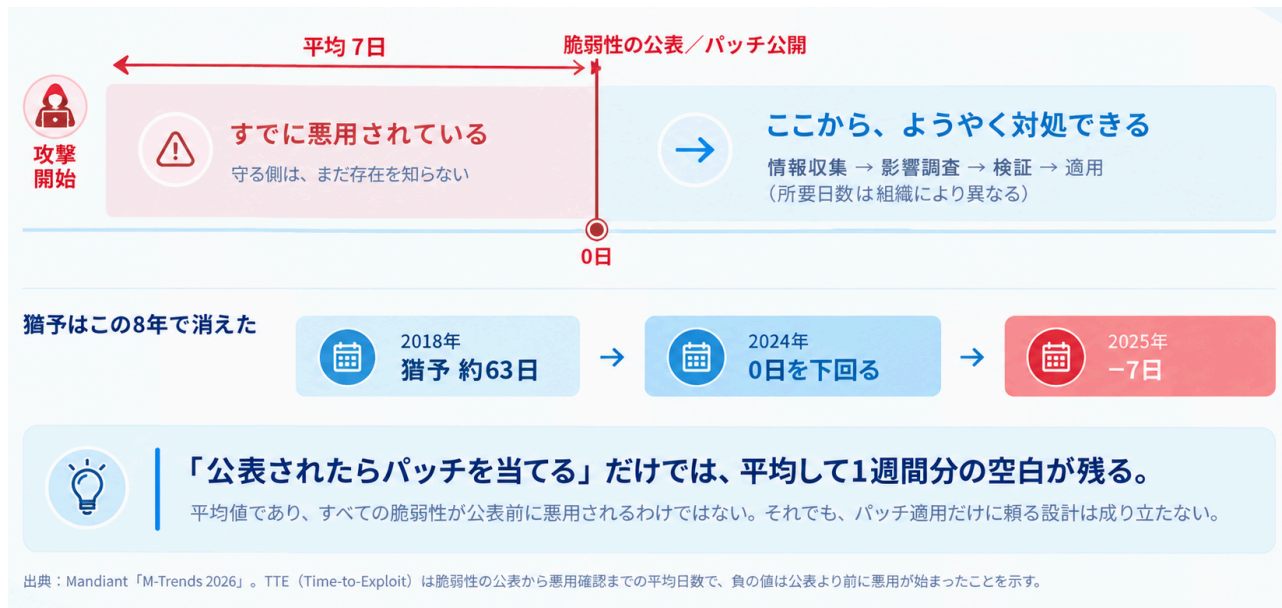
最も重要な数字：平均 TTE (Time-to-Exploit) = -7日

Mandiant 「M-Trends 2026」によれば、脆弱性の公表 (多くはパッチ公開と同時) から悪用までの平均日数は**マイナス7日**。これは「7日短くなった」という意味ではなく、**パッチが公開される平均7日前には、すでに悪用が始まっている**ということである。

推移：2018年 約63日 → 2024年に0日を下回る → 2025年 -7日。「脆弱性が公表されたらパッチを当てる」という運用は、すでに攻撃者に先行されている前提で設計し直す必要がある。

パッチは、すでに間に合っていない

脆弱性の公表から悪用までの平均日数（TTE）は-7日。攻撃は、公表される前から始まっている。



図：パッチは、すでに間に合っていない

2-2. AIが攻撃を「速く」し、必要な技能を下げた

攻撃の自動化がどこまで進んだかを示す、性質の異なる3つの報告がある。

① 能力：1年で「3分の1」から「全工程」へ

ECBのラガルド総裁は2026年10月1日のESRB年次会合で、英AI Security InstituteおよびESRB報告書を引用し、32ステップの模擬攻撃において、2025年末時点のAIモデルは平均で約3分の1のステップしか完遂できなかったのに対し、最新モデルはすべてのステップを完遂したと述べた。ESRBは、初期侵害から大規模な自動悪用までの間隔が「数週間から数時間」に短縮しうると警告している。

② 実例：2週間の工程が10時間未満に

Palo Alto Networks / Unit 42 は2026年9月2日、実際に対応したインシデントとして、複数のレッドチームが2週間かけて行う規模の侵入工程（MITRE ATT&CK 50種類以上）が、10時間未満に圧縮された事案を公表した。公開Webサービスの侵害から、内部マッピング、認証情報の収集、CI/CD乗っ取り、クラウドキー窃取までを連続実行している。注目すべきは、ゼロデイも特殊な技能も使われていない点である。

③ 兆候：自律型侵入ツールの痕跡（韓国）

2026年9月末から10月初にかけて韓国の金融7社が情報流出を公表し、新韓銀行への攻撃に使われたサーバー上に、オープンソースの自律型侵入テストツール「ARTEX AI」の痕跡が見つかったと報じられた。ただし**銀行・当局による公式確認は出ておらず、現時点では推定の域を出ない**。韓国当局も「AIが使われたのは事実だが、人間の関与なしに自律的に動いたわけではない」とコメントしている。

示唆

攻撃における希少資源が、「熟練した攻撃者の時間」から「計算資源」へ移りつつある。熟練者の時間が希少だった時代は、標的は自然と「払いの大きい相手」に絞られた。その制約が外れると、標的選定は「割に合うか」ではなく「開いているか」で決まる。

3 要因2 — 守る側の「投資の空白」

攻撃側のコストが下がる一方で、守る側、とくに中小企業の投資は増えていない。むしろ後退している。

3-1. 投資をしない企業が、10年で増えている

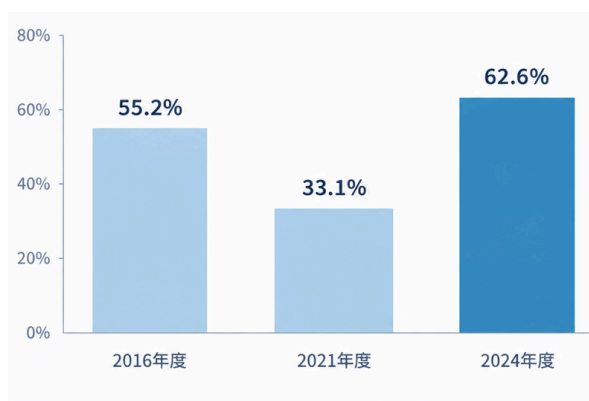
直近過去3期に情報セキュリティ投資をしていない中小企業の割合は、**2021年度の33.1%から2024年度には62.6%へと大きく増えた**（2016年度は55.2%）。投資しなかった理由の最多は「必要性を感じていない」44.3%、次いで「費用対効果が見えない」24.2%、「コストがかかりすぎる」21.7%。約7割の企業が組織的な体制を整備しておらず、専門部署を持つのは9.3%にとどまる。

3-2. 被害は、投資をしていない規模に集中している

Cisco Talos の調査によれば、2026年1～7月に国内でランサムウェア被害を受けた組織90件のうち、**資本金10億円未満が78%**（うち資本金1億円未満が48%）を占めた。2025年の69%から9ポイント上昇している。業種は製造業34%、情報通信業11%、サービス業9%。

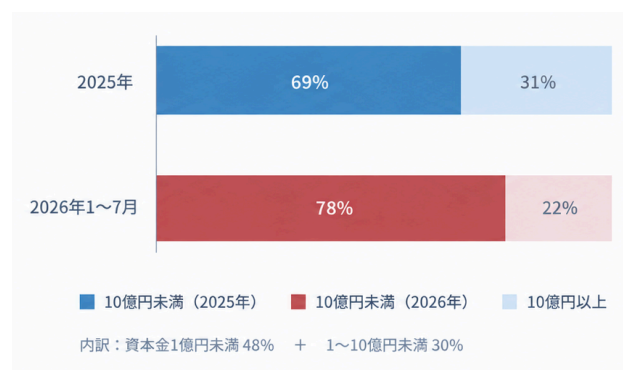
直近3期にセキュリティ投資をしていない中小企業

IPA中小企業実態調査（2024年度 n=4,191）



国内ランサムウェア被害の資本金規模

Cisco Talos（2026年1～7月 n=90）



図：投資をしない企業は増え、被害はその層に集中している

「必要性を感じていない」は、いつまで成り立つか

IPAの同調査では、被害を受けた企業の被害額は平均73万円、最大1億円、復旧までの期間は平均5.8日、最大360日と報告されている。

「必要性を感じない」という判断は、攻撃コストが高かった時代には合理的だった。攻撃者の時間が希少であれば、小規模な組織は採算が合わず後回しにされたからだ。その前提が変われば、同じ判断が同じ合理性を持つとは限らない。変わったのは判断ではなく、判断の前提のほうである。

4 要因3 — 取引先・委託先経由の侵入

IPA「情報セキュリティ10大脅威 2026」において、「サプライチェーンや委託先を狙った攻撃」は**組織向け脅威の第2位**（8年連続の選出）。2026年秋の事案は、この脅威が具体的な被害として現れた形になっている。

2026年秋には、委託先1社の侵害が複数の顧客企業に波及する事案が、2件続けて起きている。以下はその2件である。

4-1. 大和証券・シチズン時計・損保ジャパン — 委託先のサーバー1台から

影響は大和証券だけではなく。スカラコミュニケーションズは10月6日、同一サーバー上の利用企業向け環境**最大5社、最大713,126件**（問い合わせ単位の延べ件数）が対象であると公表した。自ら影響を公表したのは、大和証券（10/5・約11万名）、シチズン時計（10/6・約10万名分）、損害保険ジャパン（10/7・約6万件）、東武鉄道（10/7・形跡は確認されず）の4社である。

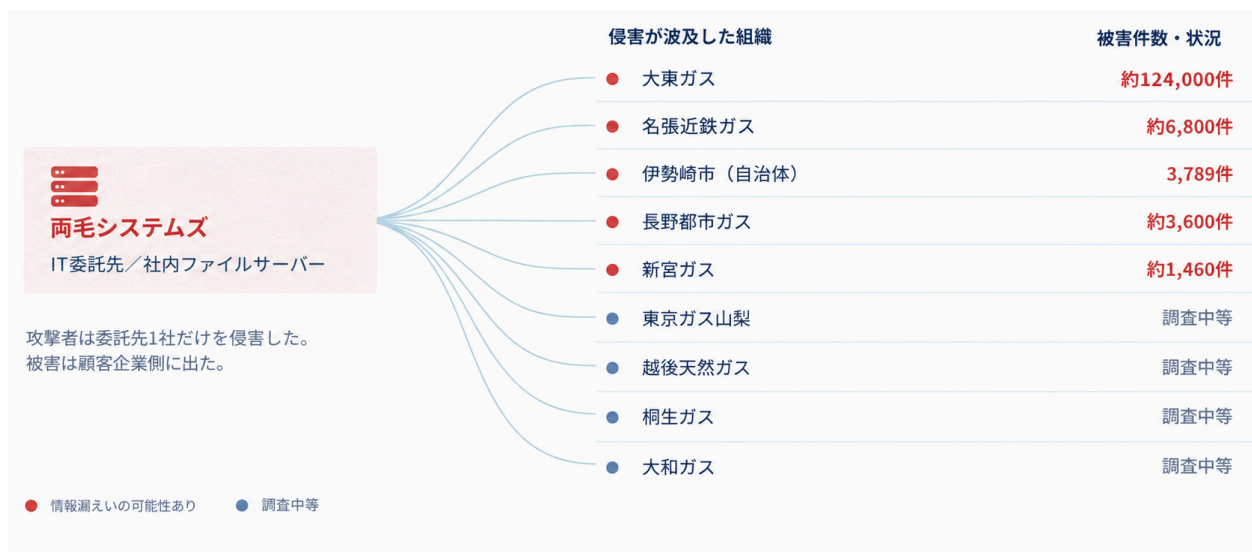
手口も公表されている。攻撃者はFAQシステム「i-ask」の管理サイトに不正ログインし、サーバー上に不正プログラムを設置したうえで、**同一サーバー上で稼働していた他の利用企業のデータベースから問い合わせ情報を取得した**。同社は再発防止策として、管理者認証の多要素化とあわせて「**環境間の分離**」を挙げている。

4-2. 両毛システムズ — 1社の侵害が9組織へ

IT企業・両毛システムズの社内ネットワークに、**8月12日にVPNアカウントを悪用して侵入され**、ファイルサーバーがランサムウェア被害を受けた。社内の死活監視で異常を検知したのは**8月14日**。同社がシステムを提供していた**ガス事業者8社と自治体1件、計9組織に影響が及んだ**。

1社の侵害が9組織へ。両毛システムの事例

8/12 VPNアカウント悪用で侵入→8/14検知



図：1社の侵害が9組織に波及した

※ 金融機関口座番号・クレジットカード情報は含まれないと公表されている。なお侵入は「通信機器の脆弱性」ではなく「VPNアカウントの悪用」と公表されており、認証情報が窃取されたのか機器側の問題かは明らかにされていない。

※ 9組織のうち漏えい件数を公表しているのは5組織（大東ガス・名張近鉄ガス・伊勢崎市・長野都市ガス・新宮ガス）で、残る4社は調査中。報道では「流出の可能性」とされている段階である。

4-3. 統計で見るサプライチェーン経由

- IPA調査で不正アクセス被害を受けた企業（n=419）のうち、**19.8%が「取引先やグループ会社等を経由して侵入された」と回答。**
- サイバーインシデントを受けた企業（n=975）の**約7割が「取引先に影響があった」と回答**（サービス停止・遅延36.1%、賠償・補償負担32.4%、原因調査・復旧の人件費負担23.2%）。
- 一方で、取引先からの要請に対応したことが**取引につながった**と回答した企業は、投資実施企業で49.8%、未実施企業で27.4%。対策は防御コストであると同時に、取引条件になりつつある。

示唆

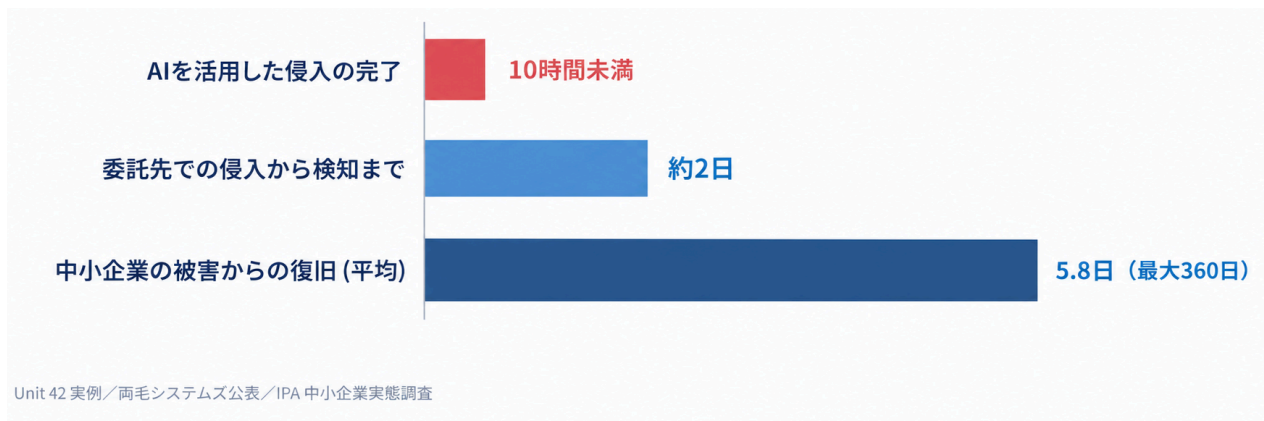
自社の防御水準は、自社の投資額では決まらない。**つながっている組織のうち最も弱いところの水準**に引き下げられる。逆に言えば、取引先に対策を求めることは「相手への負担の押し付け」ではなく自社防御の一部であり、求められる側にとっても取引継続の条件になりつつある。

5 3つが重なると何が起きるか

3つの要因は、それぞれ別の前提を壊している。どれか1つだけでも痛い、重なると打つ手が順に消える。

攻撃にかかる時間と、守る側にかかる時間

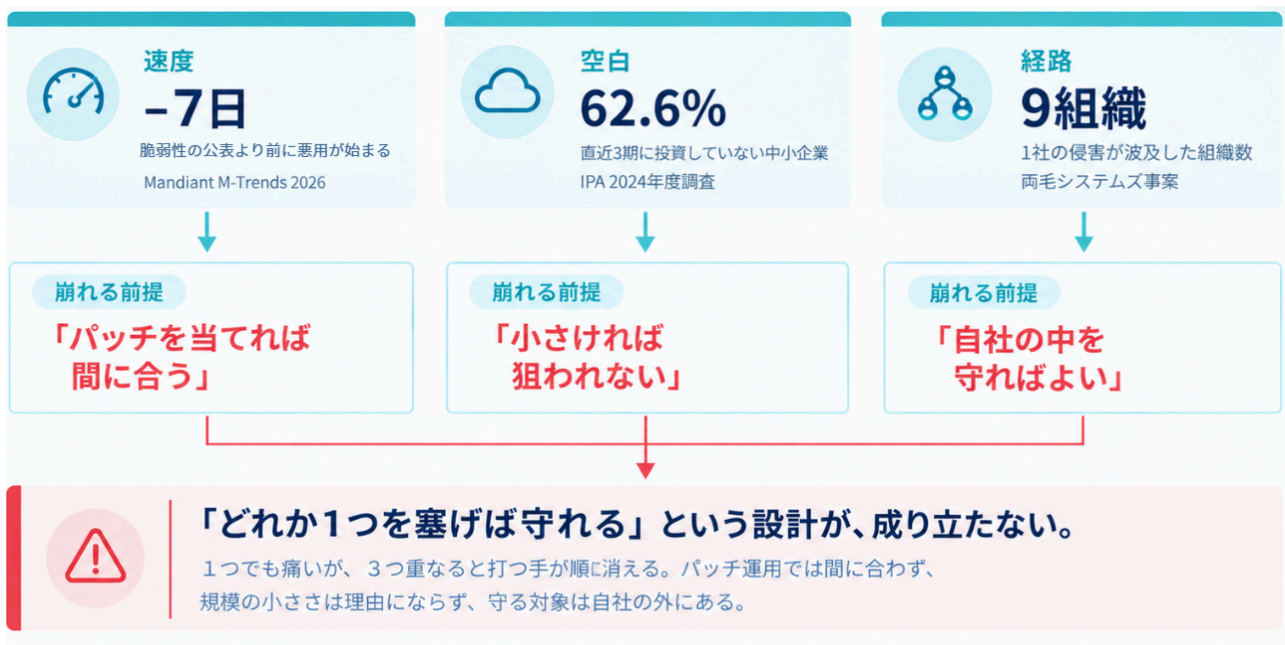
出典の異なる数値を同じ軸に並べた比較図（同一事案の時系列ではない）



図：攻撃にかかる時間と、守る側にかかる時間

守り方の前提が、3つとも外れている

3つは独立に効く。掛け合わせるのではなく、別々の前提をひとつずつ崩している



図：3つの前提が1つずつ外れている

ここで注意したいのは、この3つは出典も母集団も違うということである。-7日は世界のCVE統計、62.6%は日本の中小企業アンケート、9組織は1つの事案の波及数。掛け算して1つの数字にできるものではない。

意味があるのは、それぞれが別の防御層を無効化しているという点である。1つでも痛い、3つ重なると「どれか1つを塞げば守れる」という設計そのものが成り立たなくなる。パッチ運用では間に合わず、規模の小ささは理由にならず、守る対象は自社の外にある。

6 何から着手するか

以下は、特別な予算措置がなくても着手できる順に並べた。本章は上記の事実関係を踏まえた提言であり、各社の状況により適否は異なる。

01 棚卸しする（最優先）

外部に公開している資産、利用中のSaaS、業務を委託している先の一覧を作る。「どこに、誰の、どんな個人情報があるか」が答えられない状態では、侵害時に公表すらできない。2026年秋の事案の多くは、自社が直接管理していない場所で起きている。

02 入口を締める

VPN・リモートアクセス・各種管理画面の多要素認証（MFA）を必須化し、退職者・不要アカウントを棚卸しする。両毛システムズの事案はVPNアカウントの悪用、日本経済新聞社の事案は業務クラウドアカウントの乗っ取りが起点だった。

03 「パッチ待ち」の前提を変える

平均TTEが7日である以上、パッチ適用だけでは間に合わない時間帯が構造的に存在する。

WAFやEDRによる検知と遮断など、「侵入された後に止める」層を持つ。

※当社はWAF製品を提供しています

04 委託先を管理対象に入れる

契約にインシデント発生時の報告義務と報告期限を明記する。年1回、委託先の対策状況を確認する。取引先への要請は、自社防御の一部である。

05 公表の準備をしておく

緊急連絡体制、外部専門機関の連絡先、個人情報保護委員会への報告手順、公表文のドラフトを事前に用意する。今回の事案では、検知から第1報まで数時間～1日で公表した企業もある。公表の速さと正確さは、被害そのものと同じかそれ以上に評価される。

7 事実と推測の区分・本レポートの限界

【事実】

本文中の件数・日付・比率は、各社の公表資料、GTIG／Mandiant／Unit 42／Cisco Talos／VulnCheck のレポート、IPAの調査報告書、ECB・ESRBの公表資料に基づく。出典は下記に記載した。

【推測・留保】

- ・ **公表の集中＝攻撃の集中とは限らない**

2026年秋に公表が相次いだこと自体は事実だが、攻撃件数が同時期に急増したことを示す統計はない。個人情報保護法下での報告実務の定着や、公表判断の早期化が影響している可能性がある。

- ・ **「AIが被害増の原因」であることを定量的に示した統計は現時点では存在しない**

AIの攻撃能力向上（ESRB／英AISI、Unit 42）と被害公表の増加は、いずれも観測されている事実だが、両者の因果関係を直接示したデータは確認できなかった。本レポートでは「同時進行している」と記述するにとどめる。

- ・ **新韓銀行のARTEX AIの件は推定段階**

銀行・当局による公式確認はなく、韓国当局は「AIが人間の関与なしに自律的に動いたわけではない」としている。

- ・ **CVE公表件数の倍増は水増しを含む**

GTIG自身が生の件数は誤解を招くと注記しており、「脆弱性が2倍になった＝脅威が2倍になった」という読み方はできない。

- ・ **Talosの78%は「ランサムウェア被害を受けた組織」の内訳**

攻撃全般の統計ではない。また母数は同社が確認した90件であり、国内被害の全体像ではない。

- ・ **調査中の事案が複数含まれる**

とくにタイムズモビリティ・京王電鉄グループ・日本経済新聞社の事案は原因や被害範囲が未確定であり、今後数値が変動しうる。

出典

▼被害公表

タイムズモビリティ（パーク24グループ）

- [「タイムズカーWebシステム」への不正アクセスに関する調査結果および今後の対応について（第2報）（2026/9/28）](#)
- [同 第3報（2026/9/29）](#)
- [パーク24 ニュースリリース（2026/9/28）](#)
- [パーク24 ニュースリリース（2026/9/29）](#)

京王電鉄グループ

- [京王電鉄「ランサムウェア攻撃によるシステム障害に関するお知らせとお詫び」（2026/9/26）](#)

日本経済新聞社

- [「サイバー攻撃による情報漏洩、不審メールの送信について」（2026/10/4）](#)

第一ライフグループ／第一生命保険

- [「退職された皆さまへのお知らせ 当社の従業員向け人事システムへの不正アクセスについて」（2026/10/2）](#)

スカラコミュニケーションズの事案（大和証券ほか）

- [スカラコミュニケーションズ「FAQシステム「i-ask」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ」（2026/10/6）](#)
- [スカラ「当社連結子会社における不正アクセスによる個人情報漏えいに関するお詫びとお知らせ」（2026/10/6）](#)
- [大和証券「外部委託先への不正アクセスによるお客様情報の漏洩の可能性について」（2026/10/5）](#)
- [シチズン時計「委託先事業者に対する不正アクセスによるお客様情報の漏えいの可能性について」（2026/10/6）](#)
- [損害保険ジャパン「当社事業者向けサービスで使用する外部委託先システムへの不正アクセスによるお客さま情報漏えいの可能性について」（2026/10/7）](#)
- [東武鉄道「委託先事業者への不正アクセスについて（お知らせ）」（2026/10/7）](#)

両毛システムズの事案（大東ガスほか）

- [両毛システムズ「当社社内システムへの不正アクセスに関するお知らせ」](#)
- [長野都市ガス 第二報（2026/10/5）](#)

▼AIと脆弱性

- [Google Threat Intelligence Group「Vulnerability Discovery and Exploitation Trends in the AI Era」（2026/9/30）](#)
- [Mandiant「M-Trends 2026」（Time-to-Exploit-7日）](#)
- [同 エグゼクティブ版（PDF）](#)

- [VulnCheck「State of Exploitation 1H-2026」\(KEV入りまで中央値120日→80日\)](#)
- [Unit 42 / Palo Alto Networks「An AI-Assisted Cyber Attack: Inside a Unit 42 Investigation」\(2026/9/2\)](#)
- [Christine Lagarde「Where AI risks meet」ESRB第10回年次会合\(2026/10/1\)](#)
- [UK AI Security Institute「How fast is autonomous AI cyber capability advancing?」\(2026/5/13\)](#)
- [ESRB「Addressing frontier AI models with cyber capabilities from a financial stability perspective」\(2026/7・PDF\)](#)
- 新韓銀行の件：[Seoul Economic Daily\(2026/10/2\)](#)／[YTN\(2026/10/2\)](#)／[The Korea Times\(2026/10/5\)](#)

▼国内統計

- [Cisco Talos「2026年上半期における日本でのランサムウェア被害の状況」\(2026/9/17\)](#)
- [同 英語原文](#)
- [IPA「2024年度 中小企業における情報セキュリティ対策に関する実態調査」報告書\(2025/5公開、回収4,191件\)](#)
- [同 報告書本体\(PDF\)](#)
- [同 速報版プレスリリース\(2025/2/14\)](#)
- [IPA「情報セキュリティ10大脅威 2026」\(2026/1/29公開\)](#)

本レポートは公表済みの一次情報をもとに作成したものであり、特定の企業・製品の評価を目的とするものではありません。記載の数値は作成時点(2026年10月7日)のものです。